

REMARKS

The Applicant thanks the Examiner for an indication that the drawings filed on October 27, 200, were accepted by the Office.

The acknowledgment by the Examiner of a claim for domestic priority under 35 U.S.C. §119(e) is also noted with appreciation.

Claims 1, 3-9, 11 to 13 are currently pending in the application. By the present amendment claims 1, 3, 4, 5, 8, 12 and 13 have been amended in order to overcome the Examiner's objections and improve claim language and claims 2 and 10 have been canceled and salient recitations thereof and other claims added to independent claims. The support for the present amendment is provided at least in Figure 2 and pages 8 to 13 of the disclosure. No new matter has been added by the present amendment.

The specification has been carefully reviewed and amended to correct minor errors of idiomatic English and grammar. No new matter is added by this amendment.

The Examiner has objected the abstract as too lengthy. By the present amendment abstract has been amended in order to limit wording to the 150 words required by MPEP. The Examiner is respectfully requested to withdraw this objection in a view of the present amendment.

Claim 1 has been objected to for using the term "capable of" which as Examiner states renders claim 1 indefinite. Responding to this objection claim 1 has been amended and the expression "capable of" was deleted. Additionally, claim 10 has been objected as a substantial duplicate of claim 1. In response to this objection, claim 10 has been canceled. The Examiner is respectfully requested to withdraw the objections to the claims in a view of the present amendment.

Claims 1-13 have been rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent 6,351,813 to Mooney et al. (further Mooney et al.- I) in view of Mooney et al. (U.S. Patent 5,610,981)(further Mooney et al.-II) and in view of Schneck et al. (U.S. Patent 6,314,409). This rejection is respectfully traversed for the reason that the combination of Mooney et al.-I, Mooney et al.-II

and Schneck et al. fails to teach the invention as presently claimed.

The present invention aims to resolve a very specific problem of denying access to data secured through encryption in a combat situation or the like. The present invention is oriented to a mobile computer which can be involved in a scenario in which an adversary will seek to take possession of the computer and read the secured data and even coerce an operator to recover an encryption key. The main advantage of the present invention is that in the security control proposed by the Applicant, a so called "human factor" is brought to minimum. For instance, according to the present invention, an operator does not know the encryption key and does not need to perform additional steps to delete the key from non-volatile memory or when power is disconnected. All these give certain advantages for providing a security for the data in the combat situation. According to the present invention, an encryption function is performed by an encrypting device in the operating system and when a mission is started and the encoding/decoding key is installed only in a volatile memory. Thus, in case of power loss it will be automatically deleted. This also allows deletion of the encrypted key from non-volatile memory by a sufficiently rigorous process (e.g. overwriting a large number of times) that the encryption key cannot be recovered. Additionally, the operator has an opportunity to delete the key from volatile memory in the event of a threat, whether perceived or real. The operator does not know the key but deletion of key from volatile memory does not preclude the ongoing mission from accomplishment since non-volatile data is unencrypted. Furthermore, the method proposed by Applicant allows speeding up the process of rendering classified data unreadable within the present requirements of the U.S. government. The presently existing methods require excessive time to render the disk memory unusable by erasure overwriting and do not distinguish between classified and unclassified files. The present invention eliminates all these disadvantages.

Now specifically, referring to Figures 1 and 2, the steps of the claimed method will be explained. In the preferred embodiment of the present invention preferably two rugged commercial mass memory devices Extended Mass Storage

Unit EMSU 104 and Data Transfer System DTS 105 are installed in a mission vehicle for instance a helicopter. These devices can communicate, via a small computer system interface bus (SCSI) 101 with a Mission Computer MC 102 and A Flight Management Computer (FMC) 103 on board the mission vehicle. Unclassified tasks usually performed by FMC and MC usually deals with classified data related to a mission. According to the present invention the encryption function in the MC 102 is performed by an encrypting SCSI (Small Computer System Interface) device driver in the operating system, which passes the SCSI data through untouched or applies encryption/decryption as needed. Encrypted data on the EMSU 104 or DTS 105 is identified by an encryption flag in the file header. Classified data to be written to a storage medium 104 or 105 is delivered to the encrypting SCSI device driver in the MC where it is encrypted and transferred to EMSU 104 or DTS 105.

Referring now to Figure 2, an encryption key initially is downloaded into a mission planning workstation 201, which is located in a secure place. To set up the system, the memory medium EMSU 104 and DTS 105 are connected to the mission planning workstation 201 for downloading data. The encryption key is downloaded into EMSU 104. Further, the operator physically carries the loaded memory media and connects the EMSU 104 and DTS 105 to a mission vehicle located Mission Computer 102 and Flight Management Computer 103. When the mission vehicle is powered up, the Mission Computer loads the unclassified files, and uses the encryption key to read encrypted files. Encryption key erasure from the EMSU is triggered, for example, by the mission vehicle taking off on its mission. Thereafter, the encryption key is maintained only in volatile memory. During the further mission development an operator can erase the encryption key from volatile memory in the event of threat, whether perceived or real. Additionally, in the event of power disconnection the encryption key is going to be deleted as well as the rest of content of RAM memory. Encrypted data in non-volatile memory is thus protected. However, even if the encryption key is deleted from volatile memory non-classified data needed for completing of mission can be

retrieved since it is not encrypted.

As it can be seen from the above description the present invention provides the following advantages of security of mission related data:

the present invention does not require authentication of a user;

the mission computer 102 and flight management computer 103 do not have a direct access to the Mission Planning Workstation 201 during a mission, because the information related to the current mission is downloaded and after that the connection terminated;

the encryption key is stored in the Extended Mass Storage Unit 104 (non-volatile memory) only for a period before the mission starts, after that it is deleted out from the non-volatile storage, and installed only in volatile memory;

in the case of threat, the encryption key can be easily deleted from volatile memory;

an operator does not know an encryption key, so in the event of his/her being captured during a mission, the operator can not reveal it.

The reference to Mooney et al.-I is related to protecting and controlling access to data from theft using a system of electronic keys and a smart card. Mooney et al.-I aims to provide an access to a crypto system using a number of smart cards. It is known that a smart card is a tamper-resistant hardware device with a microprocessor which in the present application contains a private keys and other sensitive information for a particular user. In other words, a smart card allows determination if a user is authorized to access the computer or not. According to Mooney et al.-I a user by himself/herself can choose the level of security. Therefore, the Mooney et al.-I uses encryption and smart card technology to control security and provide a sophisticated access hierarchy for varying levels of security to various classes of users.

Referring to Figure 3A in Mooney et al.-I, the proposed software program execution will be explained. Before a system is provided to the user, a smart card preparation program is run in order to initialize the smart card access codes, create necessary smart card files including session key files, level files and data files,

initialize those files with level key data. Upon receiving the system, the user changes the default questions and answers to the questions. The system can provide several levels of security selected by the user. First, prior to a software execution the security check by a smart card is performed. The user answers a number of questions in order to get an access to the system. Next, the user begins executing the software in step 320. During execution of this step a user has an option of creating a new key for encryption/decryption 330 or selecting a previously created key from the smart card. Next, the encrypt and decrypt functions may be carried out on the source files as shown in step 370. After the selected encrypt or decrypt functions are finished, the user may either go back to the beginning and create a new key or select an existing key, or terminate the software program. Therefore, the system to Mooney et al. -I provides a good protection from theft. It utilizes features of the smart card to authenticate users while incorporating multiple levels of security. After authentication the user is granted access to a database which stores objects such as electronic keys. Conveniently, to a variety of resources the electronic keys may be stored on the smart card too. However, these functions are of little if any relevance to the present invention, as claimed for the simple reason that the operator of Mooney wt al. must know the encryption keys or access authorization information while the present invention provides for such information to be unknown to the operator.

More specifically, it can be seen, the Applicant's system and Mooney's resolve the problem of access of unwanted person to the computer data by different ways due to the different circumstances of usage. The Applicant has developed his system for a combat situation wherein in the event of a threat the encryption key from volatile memory will be deleted. It is assumed that during a mission there is always a risk that an operator could be captured and coerced into revealing the passwords or keys if known. The encryption function in the present invention is performed by Small Computer System Interface bus driver in the operating system. This device driver either passes the SCSI data through untouched or applies encryption or decryption to the data as needed. That is why the

encryption/decryption keys in the present invention are stored only in volatile memory in order to be easy deleted in the event of threat perceived or real or in case of power disconnection. Additionally, an operator in the system proposed by Applicant does not know the keys which provides the distinct advantage that the encryption key cannot be coerced from a human and entered into the portable system by unauthorized personnel. Due to the special usage, the present invention constructively comprises mission planning workstation 201, which is located into the secure place, and mission computer 102, which is provided at the helicopter or ship taking part in the mission. According to the Applicant unencrypted sensitive data is never placed in non-volatile storage, which means that if the device is powered off there is no chance of any compromise of data. On other hand since the key is not stored in permanent or non-volatile memory, there is never a case when the system can be disabled at a time before the key is erased, once it has left the base area on a mission.

As it can be seen the system proposed by Mooney et al.-I addresses needs of a more casual user who is not in a military operation. According to Mooney et al.-I, the encryption/decryption keys are stored on a smart card. The smart card also is used to authenticate a user. In Mooney et al.-I the user has knowledge of keys and preselect them by himself as well as selecting and setting up the level of security.

The reference to Mooney et al. (U.S. Patent 5,610,981), hereinafter Mooney et al.-II also teaches a secure computer controlling access to data storage devices via a card reader. The card reader interface includes an encryption engine for encrypting data in a data storage device and a boot ROM containing verification program code executed during an initialization code executed during an initialization procedure. A user is denied access if he/she cannot provide correct answers during authorization verification by freezing the system bus, logically destroying the data in the data storage devices or physically destroying the data storage devices. The system to Mooney et al.-II monitors attempted unauthorized retrieval of data from the protected storage devices and present information to processor if unauthorized access is detected. The processor in its turn issues a

command to either logically or physically destroy protected information in RAM or secure hard drive. Specifically, Mooney et al.-II states, "Logical destruction of data on the RAM 260 is accomplished by asserting trigger signal 211 emanating from processor 220, clearing the contents of RAM 260. " (Column 8, lines 45 *et seq.*) As it can be seen the elimination of the data in RAM according to Mooney et al.-II is initiated automatically when an authorization verification fails. In contrast, according the present invention, an encryption key is deleted from non-volatile memory when it is transferred to volatile memory and can be deleted from volatile memory or by an operator in event of a threat or automatically when power goes off. There is no authorization verification in the present invention and there is no command from processor to logically or physically destroy protected information in RAM. Moreover, the Applicant provides elimination of an encryption key from RAM due to power outage, whereas the invention to Mooney et al.-II has a battery to provide uninterrupted power even in case of outage. As it already was highlighted, the present invention is created for a combat environment, wherein an operator does not have any knowledge of classified data and security of classified data should be provided almost automatically. This is quite different from the method to Mooney et al.-II, wherein a failed authorization triggers clearing up of RAM. In the present invention clearing of RAM can be manually initiated by the operator or automatically done due to power outage.

It should be respectfully noted that a crucial distinction between the present invention and both Mooney's patents resides in the authentication required in Mooney which is not necessary and avoided according to the present invention. The present invention provides the method in accordance with which an operator does not need to authenticate himself/herself because when encrypted classified and non-encrypted non-classified data are downloaded into a mission vehicle board computer it takes place in a friendly territory and after a mission is started any threat will initiate erasure of an encryption key and inaccessibility of classified data for an operator himself as well to any unwanted potential user. Therefore, the Examiner's attempt to combine both Mooney's patents generally creates a method

absolutely opposite to the Applicant's method, which teaches avoiding the authentication by a user. Further, citing *In re Gordon et al.*, 221 USPQ 1125 (Fed. Circ., 1984), Applicant submits that Mooney's patents cannot be used to support a *prima facie* obviousness rejection based on 35 U.S.C. §103 because "it would be rendered inoperable for its intended purpose" if modified to answer the subject matter of the claims.

The Examiner also relied on the reference to Schneck et al. as providing a degree of protection in accordance with nature of the data as well as the user environment. The patent to Schneck et al. shows the system which provides a control of access to data in accordance to rules concerning access rights to the data. In the office action the Examiner relies on column 7, lines 4-22 in Schneck et al. as describing the identical invention. Particularly, Schneck et al. describes the preferred embodiment the following way, "...a method of controlling access to data by protecting portions of the data; determining rules concerning access rights to the data; preventing access to the protected portions of the data other than in a non-usable form; and permitting a user access to the data only in accordance with the rules as enforced by a tamper detecting mechanism." (Emphasis added to show the features not presented by the present invention.) Moreover, the issue presented by the invention relative to the combined teachings of Mooney is the kind of protection provided rather than the degree of protection provided. Modification of the combined teachings of the Mooney references which are directed to providing an entirely different kind of protection irrelevant to the invention and directed to providing a function avoided by the invention cannot be shown to be obvious by teaching of Schneck et al. directed to altering the degree of the same kind of protection. Rather, the Examiner's application of Schneck et al. tends to emphasize the fact that the kind of protection provided by separate or combined teachings of Mooney is altogether insufficient to the degree of protection provided by the invention in avoiding the need for a user to know information by which data is protected.

To emphasize the distinction, claims 1 and 12 have been amended.

Specifically, claim 1 as amended recites, “...loading an encryption key into a mission planning workstation at a first location;

connecting a media device to said mission planning workstation

loading said encryption key from said mission planning workstation into said media device; ...

transferring said encryption key to volatile memory from said media device;

deleting said encryption key from said media device upon said land, air, space or sea vehicle taking off;

maintaining said encryption key only in volatile memory after said deleting step; and ...

whereby said target portable computing device operator has no knowledge of encryption key.” (Emphasis added) It should be noted that essentially limitations of claims 2 and 4 have been incorporated in claim 1 and subsequently claim 2 has been canceled and claim 4 amended. As amended, it is submitted that independent claims 1 and 12 clearly defines over the patent to Mooney et al.-I, Mooney et al.-II and Schneck et al.

Summarizing the above arguments and amendment the Applicant one more time highlights the features of the present invention which is not shown by the prior art relied on by the Examiner:

the present invention does not require authentication of a user;

the mission computer 102 and flight management computer 103 do not have a direct access to the Mission Planning Workstation 201 during a mission, because the information related to the current mission is downloaded and after that the connection terminated;

the encryption key is stored in the Extended Mass Storage Unit 104 (non-volatile memory) only for a period before the mission starts, after that it is deleted out from the non-volatile storage, and installed only in volatile memory;

in the case of threat encryption key can be easily deleted from volatile memory;

an operator does not know an encryption key, so in the event of his/her

capturing during a mission and coercing into revealing the key, the operator simply cannot reveal it. These meritorious functions are fully supported by the subject matter of the claims and are not realized by the prior art relied on by the Examiner.

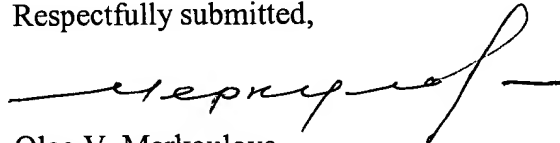
The prior art cited but not relied on by the Examiner has been reviewed, but for the reasons already advanced, that prior art is similarly not relevant to the invention as now claimed.

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 1, 3-9, 11-13 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 50-2041 (Whitham, Curtis & Christofferson, P.C.).

Respectfully submitted,



Olga V. Merkoulouva
Registration No. 48,757

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190
Tel. (703) 787-9400
Fax. (703) 787-7557
Customer No.: 30743